Commentaire

Décision n° 2021-976/977 QPC du 25 février 2022

M. Habib A. et autre

Question prioritaire de constitutionnalité portant sur les paragraphes II et III de l'article L. 34-1 du code des postes et des communications électroniques

(Conservation des données de connexion pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales)

Le Conseil constitutionnel a été saisi le 10 décembre 2021 par la Cour de cassation (chambre criminelle, arrêts n[os] 1590 et 1591 du 7 décembre 2021) de deux questions prioritaires de constitutionnalité (QPC) posées par M. Habib A. et M. Samy B. relatives à la conformité aux droits et libertés que la Constitution garantit des paragraphes II et III de l'article L. 34-1 du code des postes et des communications électroniques (CPCE), dans sa rédaction résultant de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

Dans sa décision n° 2021-976/977 QPC du 25 février 2022, le Conseil constitutionnel a déclaré contraires à la Constitution les mots *« la recherche, de la constatation et de la poursuite des infractions pénales »* et *« de l'autorité judiciaire ou »* figurant à la première phrase du paragraphe III de l'article L. 34-1 du CPCE, dans cette rédaction.

I. – Les dispositions contestées

A. – Objet et évolution des dispositions contestées

1. – Le régime applicable à la conservation et à l'accès aux données de connexion

L'utilisation par une personne d'appareils de communications électroniques laisse des traces numériques, communément désignées « données de connexion » ou « métadonnées » pour les distinguer des données portant sur le contenu des communications.

Sous cette expression générique, la loi appréhende de nos jours trois catégories de données distinctes :

– les données d'identité civile de l'utilisateur d'un moyen de communication électronique (par exemple les nom et prénom liés à un numéro de téléphone ou à une adresse IP) ;

– les données relatives au trafic, qui sont définies au 18° de l'article L. 32 du CPCE comme *« toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou en vue de sa facturation »*. Ces données désignent, plus concrètement, les informations techniques générées par l'utilisation des réseaux de communications électroniques tels qu'internet[1]. Il s'agit par exemple, dans le cas de communications réalisées à partir d'un ordinateur connecté à internet, de l'adresse IP de l'ordinateur, de la date, de l'heure et de la durée de chaque connexion ou encore de l'adresse des sites internet consultés ; dans le cas de communications réalisées à partir d'un téléphone, ces données regroupent les informations sur les communications d'une ligne téléphonique, parfois appelées « fadettes » (par exemple le numéro de téléphone appelé, la date, l'horaire et la durée de l'appel). Les données de trafic peuvent permettre, selon les cas, d'identifier indirectement l'utilisateur du terminal ainsi que le destinataire de la communication ;

– les données de localisation, qui permettent d'identifier l'origine de la communication et la position géographique du terminal et qui résultent, par exemple, du « bornage » d'un appareil mobile sur l'antenne relais à laquelle il s'est connecté.

Compte tenu de l'utilisation massive des appareils électroniques dans la vie quotidienne, ces données ont pris une importance croissante dans le recueil d'informations par les services de renseignement ainsi que les autorités judiciaires et administratives autorisés à y accéder pour les besoins de leurs investigations, que ce soit pour reconstituer les déplacements d'une personne, identifier ses contacts ou ses centres d'intérêts.

Le risque d'atteinte à la vie privée que recèlent ces données a conduit le législateur à prévoir des règles relatives à leur conservation ainsi qu'à leur accès.

[1] https://www.cnil.fr/fr/conservation-des-donnees-de-trafic-hot-spots-wi-fi-cybercafes-employeurs-quelles-obligations.

a. – La conservation des données de connexion (les dispositions objet de la décision commentée)

* Les règles relatives à la conservation des données de connexion sont déterminées par l'article L. 34-1 du CPCE[2].

Ces dispositions, qui figuraient initialement à l'article L. 32-3-1 du code des postes et télécommunications[3], sont issues de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne. L'encadrement de la conservation des données était destiné *« à ce que les autorités judiciaires ne soient pas tributaires des données conservées par les opérateurs pour leurs besoins propres, selon les choix commerciaux qu'ils auront fait »*[4]. Conformément à la directive 97/66/CE du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, ces dispositions prévoyaient, pour ces opérateurs, l'obligation d'effacer et de rendre anonymes les données de trafic dès que la communication est terminée. Dans un contexte marqué par les attentats ayant frappé les États-Unis le 11 septembre 2001, elles instituaient en outre un régime d'exception pour la conservation de ces mêmes données pour sauvegarder la sûreté de l'État, la défense, la sécurité publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales.

* L'article L. 34-1 du CPCE[5] s'applique au traitement des données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques. Il prévoit, d'une part, l'obligation de principe pour les opérateurs de communications électroniques de supprimer les données de connexion et, d'autre part, des exceptions à cette obligation.

Ainsi, aux termes du premier alinéa du paragraphe II, *« Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic »*, sous réserve des exceptions prévues aux paragraphes suivants.

Le deuxième alinéa du paragraphe II de l'article L. 34-1 du CPCE contraint par ailleurs les personnes qui fournissent au public des services de communications

[2] D'autres dispositions imposent par ailleurs la conservation des données permettant l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus en ligne. Elles sont prévues à l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

[3] Devenu article L. 34-1 du CPCE par la loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle.

[4] Amendement n° 9 présenté par le Gouvernement le 6 octobre 2001 lors de la discussion en séance publique du projet de loi devant le Sénat.

[5] Dans sa version résultant de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

électroniques à établir des procédures internes permettant de répondre aux demandes des autorités compétentes.

Le troisième alinéa étend cette obligation aux personnes qui offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit.

Le paragraphe III de ce même article prévoit que, par dérogation à l'obligation d'effacement ou d'anonymisation des données, les opérateurs de communications électroniques peuvent être tenus de différer pour une durée maximale d'un an les opérations d'effacement ou d'anonymisation de certaines catégories de données techniques.

Ce report peut intervenir pour trois finalités :

– la recherche, la constatation et la poursuite de toutes les infractions pénales ;

– la recherche, la constatation et la poursuite par la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (Hadopi[6]) du manquement par la personne titulaire de l'accès à un service de communication au public en ligne à son obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ;

– la prévention par l'Agence nationale de sécurité des systèmes d'information (ANSSI) des atteintes aux systèmes de traitement automatisé de données.

La loi renvoie à un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés (CNIL), la détermination des catégories de données concernées et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'État, par les opérateurs[7].

* En application du paragraphe VI de l'article L. 34-1 du CPCE, ces données *« portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des*

[6] Ses missions sont désormais assurées, comme celles du Conseil supérieur de l'audiovisuel, par l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM).

[7] Il faut ajouter la possibilité, pour les opérateurs, prévue par le paragraphe IV de l'article L. 34-1 du CPCE, de conserver les données nécessaires aux besoins de la facturation et du paiement des prestations de communications électroniques.

communications assurées par ces derniers et sur la localisation des équipements terminaux. / Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications ».

Le même paragraphe ajoute, *in fine*, que *« La conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés »* et que les opérateurs prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues à l'article L. 34-1.

* L'article R. 10-13 du CPCE[8] dresse la liste des données conservées par les opérateurs de communications électroniques pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales. Il s'agit, en ce qui concerne les activités numériques :

– des informations permettant d'identifier l'utilisateur ;

– des données relatives aux équipements terminaux de communication utilisés ;

– des caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;

– des données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;

– des données permettant d'identifier le ou les destinataires de la communication ;

– ainsi que des données permettant d'identifier l'origine et la localisation de la communication.

Pour les activités de téléphonie, il est en outre prévu que l'opérateur conserve les données permettant d'identifier l'origine et la localisation de la communication.

La durée de conservation de ces données est d'un an à compter du jour de l'enregistrement.

* Le 2° du paragraphe I de l'article L. 39-3 du CPCE punit d'un an d'emprisonnement et de 75 000 euros d'amende le fait pour un opérateur de communications électroniques ou ses agents de ne pas procéder à la conservation

[8] Dans sa rédaction résultant du décret n° 2012-436 du 30 mars 2012 portant transposition du nouveau cadre réglementaire européen des communications électroniques.

des données techniques dans les conditions où cette conservation est exigée par la loi.

b. – L'accès aux données de connexion

* Les données de connexion sont accessibles aux autorités visées au paragraphe III de l'article L. 34-1 du CPCE, c'est-à-dire l'autorité judiciaire[9], la Hadopi et l'ANSSI dans le cadre de leurs missions respectives.

En outre, par le jeu de dispositions spécifiques renvoyant à cet article L. 34-1, peuvent notamment avoir accès aux données de connexion, à des fins répressives :

– les enquêteurs de l'Autorité des marchés financiers (AMF) pour la recherche des abus de marché, sur autorisation préalable d'un contrôleur des demandes de données de connexion[10] ;

– les enquêteurs de l'Autorité de la concurrence pour la recherche et la constatation des pratiques anticoncurentielles, sur autorisation préalable du rapporteur général de l'Autorité de la concurrence ou de l'autorité administrative chargée de la concurrence et de la consommation auprès d'un contrôleur des demandes de données de connexion[11] ;

– les agents des douanes ayant au moins le grade de contrôleur et spécialement habilités par le directeur du service auquel ils sont affectés, pour constater certains délits douaniers[12] ;

– les agents de contrôle de l'inspection du travail pour les données permettant l'identification des personnes proposant un travail, une prestation ou une activité pouvant relever des infractions constitutives de travail illégal[13] ;

– les agents de l'administration des impôts, pour les besoins de la recherche ou de la constatation de certaines infractions de nature fiscale[14] ;

* Les services de renseignement bénéficient d'un droit de communication de ces données à des fins préventives, dans le cadre de l'accès administratif aux données

[9] Par le biais des réquisitions prévues aux articles 60-1 et 60-2 du code de procédure pénale (pour l'enquête de flagrance), 77-1-1 et 77-1-2 du même code (pour l'enquête préliminaire) ainsi que 99-3 et 99-4 du même code (pour l'information judiciaire).
[10] Article L. 621-10-2 du code monétaire et financier. Ce contrôleur des demandes de données de connexion est, en alternance, un membre du Conseil d'État, puis un magistrat de la Cour de cassation.
[11] Article L. 450-3-3 du code de commerce.
[12] Article 65 *quinquies* du code des douanes.
[13] Article L. 8113-5-2 du code du travail.
[14] Article L. 96 G du livre des procédures fiscales.

de connexion. Cet accès peut avoir lieu en temps différé[15], sur autorisation préalable du Premier ministre, délivrée après avis de la Commission nationale de contrôle des techniques de renseignement. Il peut aussi avoir lieu en temps réel. Dans ce cas, l'accès a lieu pour les seuls besoins de la prévention du terrorisme et l'autorisation est délivrée à titre individuel à un seul agent[16].

2. – Les exigences du droit de l'Union européenne en matière de protection des données de connexion et leur réception en droit interne

L'article 15 de la directive 2002/58/CE du 12 juillet 2002, dite *« vie privée et communications électroniques »*[17], a permis aux États membres d'adopter des mesures législatives dérogeant à l'obligation d'effacement des données personnelles posée, par ailleurs, par ce texte *« lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électronique »*.

La Cour de justice de l'Union européenne (CJUE) est intervenue à plusieurs reprises pour préciser les exigences du droit de l'Union protégeant le traitement des données de connexion.

* Dans son arrêt *Digital Rights Ireland Ltd* du 8 avril 2014[18], elle a d'abord invalidé une directive spécifique de 2006, dite *« conservation des données de connexion »*[19], qui prévoyait que les États membres devaient obliger les opérateurs à conserver de telles données entre six mois et deux ans en vue de leur exploitation à des fins de recherche, de détection et de poursuites d'infractions graves.

Cette obligation de conservation des données de connexion était contestée dans plusieurs États membres. Sa transposition avait donné lieu à plusieurs décisions de juridictions suprêmes annulant les mesures nationales qui devaient en assurer l'application en droit interne[20].

---

[15] Article L. 851-1 du code de la sécurité intérieure.
[16] Article L. 851-2 du code de la sécurité intérieure.
[17] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.
[18] CJUE, grande chambre, 8 avril 2014, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a.*
[19] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.
[20] Cour constitutionnelle allemande, arrêts du 2 mars 2010, BVerfGE 118,79 ; Cour constitutionnelle roumaine, arrêt du 8 octobre 2009, n° 1.258 ; Cour constitutionnelle tchèque, arrêt du 22 mars 2011, Pl. US 24/10.

Dans cet arrêt, la CJUE a relevé que les données relatives au trafic et les données de localisation *« permettent, notamment, de savoir quelle est la personne avec laquelle un abonné ou un utilisateur inscrit a communiqué et par quel moyen, tout comme de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu. En outre, elles permettent de connaître la fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une période donnée. / Ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci »*[21].

Dans de telles circonstances, elle a considéré que même si la directive examinée n'autorisait pas la conservation du contenu de la communication et des informations consultées en utilisant un réseau de communications électroniques, mais seulement des données de connexion, il n'était pas pour autant exclu *« que la conservation des données en cause puisse avoir une incidence sur l'utilisation, par les abonnés ou les utilisateurs inscrits, des moyens de communication visés par cette directive et, en conséquence, sur l'exercice par ces derniers de leur liberté d'expression, garantie par l'article 11 de la Charte »*[22].

La CJUE a relevé qu'en l'espèce, la directive ne prévoyait pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, et qu'elle comportait donc *« une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire »*[23].

* Par la suite, dans un arrêt *Tele2 Sverige AB* du 21 décembre 2016[24], la CJUE a jugé que l'article 15, paragraphe 1, de la directive *« vie privée »* du 12 juillet 2002, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés

[21] CJUE, décision du 8 avril 2014 précitée, § 26-27.
[22] *Ibid.*, § 28.
[23] *Ibid.*, § 65.
[24] CJUE, grande chambre, 21 décembre 2016, affaires jointes C-203/15 et C-698/15, *Tele2 Sverige AB c/ Post-och telestyrelsen, et Secretary of State for the Home Department c/ Tom Watson, Peter Brice, Geoffrey Lewis*.

et utilisateurs inscrits concernant tous les moyens de communications électroniques.

La Cour a rappelé que, *« prises dans leur ensemble, ces données sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci […]. En particulier, ces données fournissent les moyens d'établir […] le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications »*[25].

Elle a ajouté que l'ingérence résultant d'une réglementation nationale prévoyant la conservation des données relatives au trafic et des données de localisation *« s'avère d'une vaste ampleur et doit être considérée comme particulièrement grave. La circonstance que la conservation des données est effectuée sans que les utilisateurs des services de communications électroniques en soient informés est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante »*[26]. Par conséquent, seule la lutte contre la criminalité grave est susceptible de justifier une telle ingérence.

Pour la Cour, une réglementation prévoyant une conservation généralisée et indifférenciée des données *« ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique. Notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique et/ou sur un cercle de personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité »*[27].

Une telle réglementation nationale excède donc les limites du strict nécessaire et ne saurait être considérée comme étant justifiée dans une société démocratique, ainsi que l'exige la directive lue à la lumière de la Charte.

[25] *Ibid.*, § 99.
[26] *Ibid.*, § 100.
[27] *Ibid.*, § 106.

* Au regard de ses implications pour les États membres, cet arrêt a donné lieu à une réaction de la part de certaines de leurs juridictions qui ont tenté d'inciter la Cour à infléchir sa position[28].

En ce sens, par une décision du 26 juillet 2018[29], le Conseil d'État a saisi la CJUE de la question préjudicielle suivante : *« L'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive du 12 juillet 2002, ne doit-elle pas être regardée, notamment eu égard aux garanties et contrôles dont sont assortis ensuite le recueil et l'utilisation de ces données de connexion, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte des droits fondamentaux de l'Union européenne et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États-membres en vertu de l'article 4 du traité sur l'Union européenne ».*

En réponse, dans son arrêt *La Quadrature du Net et autres* du 6 octobre 2020[30], la CJUE a confirmé et précisé sa jurisprudence, opérant une distinction selon les catégories de métadonnées et les finalités de leur conservation.

Elle a ainsi jugé que le droit de l'Union s'oppose par principe à des mesures législatives prévoyant, aux fins prévues à cet article 15, paragraphe 1, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation.

Elle a toutefois précisé que le droit de l'Union ne s'oppose pas à des mesures législatives permettant :

– aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. La CJUE ajoute que la décision prévoyant cette injonction doit pouvoir faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, et qu'elle ne peut être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace ;

[28] Jurisprudence confirmée quelques mois plus tard par la Cour dans un nouvel arrêt (CJUE, grande chambre, 2 octobre 2018*, Ministerio Fiscal*, C-207/16).
[29] Conseil d'État, 26 juillet 2018, *La Quadrature du Net et autres*, n[os] 394922, 394925, 397844, 397851.
[30] CJUE, grande chambre, 6 octobre 2020, affaires jointes C-511/18, C-512/18 et C-520/18, *La Quadrature du Net et autres.*

– aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable[31] ;

– aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ;

– aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques ;

– aux fins de la lutte contre la criminalité grave et, *a fortiori*, de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques, par le biais d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services.

* À la suite de la réponse apportée par la CJUE à ses questions préjudicielles[32], le Conseil d'État a statué au fond sur les requêtes de plusieurs associations et fournisseurs d'accès à internet, tendant à l'annulation pour excès de pouvoir de dispositions réglementaires, et notamment de l'article R. 10-13 du CPCE dressant la liste des données devant être conservées par les opérateurs de communications

[31] Dans son arrêt *H. K. / Prokuratuur* du 2 mars 2021 (C-746/18), la Cour de justice a par ailleurs affiné les exigences découlant du droit au respect de la vie privée en matière de recours aux techniques de surveillance numériques à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales. S'agissant de la nature et de la quantité des données de connexion susceptibles d'être recueillies et de la durée pendant laquelle leur recueil était possible, la CJUE a insisté sur le fait que *« l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte l'accès, par une autorité publique, à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise, présente en tout état de cause un caractère grave indépendamment de la durée de la période pour laquelle l'accès auxdites données est sollicité et de la quantité ou de la nature des données disponibles pour une telle période, lorsque […] cet ensemble de données est susceptible de permettre de tirer des conclusions précises sur la vie privée de la ou des personnes concernées »* (§ 39).

[32] À noter qu'une question préjudicielle a été posée par la Cour de cassation à la CJUE, relative à la conservation généralisée et indifférenciée des données de connexion pour permettre à l'Autorité des marchés financiers de détecter les manquements d'initiés ou les manipulations de marché (Cass. crim., 1er avril 2020, n° 19.80.908).

électroniques pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales.

Dans sa décision du 21 avril 2021[33], le Conseil d'État a, tout d'abord, précisé le cadre de son contrôle.

D'une part, il a refusé d'opérer un contrôle de l'*« ultra vires »* qui aurait consisté à vérifier que les organes de l'Union européenne, et notamment la CJUE, n'avaient pas excédé leurs compétences. D'autre part, après avoir rappelé que la Constitution française demeure la norme suprême du droit national, il a jugé qu'il lui revenait en conséquence de vérifier que l'application du droit européen, tel que précisé par la CJUE, ne compromet pas en pratique des exigences constitutionnelles qui ne sont pas garanties de façon équivalente par le droit européen.

En l'espèce, le Conseil d'État a jugé que les objectifs de valeur constitutionnelle de sauvegarde des intérêts fondamentaux de la Nation, de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions pénales et de lutte contre le terrorisme *« ne sauraient être regardées comme bénéficiant, en droit de l'Union, d'une protection équivalente à celle que garantit la Constitution »*. Il en a déduit qu'il devait donc s'assurer que les limites définies par la CJUE ne mettent pas en péril ces exigences constitutionnelles.

C'est donc à cette aune que le Conseil d'État a examiné les dispositions réglementaires relatives à la conservation des données de connexion. Il a constaté que le législateur a entendu imposer aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs l'obligation de conserver de manière générale et indifférenciée les données de connexion pour les besoins, d'une part, de la recherche, de la constatation et de la poursuite des infractions, notamment pénales, et, d'autre part, des missions de défense et de promotion des intérêts fondamentaux de la Nation confiées aux services de renseignement[34].

– S'agissant de la conservation générale et indifférenciée des adresses IP, le Conseil d'État a considéré que, même *« si la conservation généralisée et indifférenciée des adresses IP ne saurait être justifiée par les besoins de la lutte contre l'ensemble des infractions pénales »*, une telle obligation peut ainsi être imposée aux opérateurs, dès lors que les conditions d'accès à ces données par les services d'enquête sont fixées en fonction de la gravité des infractions susceptibles de le justifier, dans le respect du principe de proportionnalité. Il a

[33] Conseil d'État, Assemblée, 21 avril 2021, n° 393099, Publié au recueil Lebon, points 3 à 10.
[34] *Ibid.*, point 20.

ainsi jugé que les dispositions réglementaires applicables – notamment l'article R. 10-13 du CPCE – ne sont pas contraires au droit de l'Union européenne[35].

– S'agissant de la conservation générale et indifférenciée des données de trafic et de localisation autres que les adresses IP, le Conseil d'État a jugé que la conservation générale et indifférenciée des données de connexion aux fins de sauvegarde de la sécurité nationale était, en l'état, justifiée par les menaces pour la sécurité nationale qui pèsent actuellement sur la France. Afin de respecter toutefois les exigences résultant de l'arrêt précité du 6 octobre 2020 de la CJUE, il n'a annulé les dispositions règlementaires dont il était saisi, et notamment l'article R. 10-13 du CPCE, qu'en tant qu'elles ne subordonnaient pas le maintien en vigueur de l'obligation de conservation générale et indifférenciée au constat à échéance régulière de la persistance d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale. Puis, constatant qu'une telle menace existait à la date de sa décision, il a maintenu en vigueur ces dispositions réglementaires et donné un délai de six mois au Gouvernement pour compléter en ce sens les dispositions règlementaires[36].

Le Conseil d'État a en revanche constaté l'incompatibilité avec les exigences européennes de l'obligation de conservation généralisée de ces données sensibles pour les besoins autres que ceux de la sécurité nationale, notamment la recherche des infractions pénales. Toutefois, avant de juger cette conservation incompatible avec les exigences européennes, il s'est assuré que les conséquences de cette incompatibilité ne privaient pas de garanties effectives les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public, notamment des atteintes à la sécurité des personnes et des biens, et de recherche des auteurs d'infractions pénales.

Pour la recherche de telles infractions, il a tout d'abord relevé que *« L'accès différé aux données de connexion revêt une importance d'autant plus cruciale que l'utilisation des moyens de communications électroniques, notamment cryptées, constitue un instrument qui facilite la commission de ces crimes et délits et rend plus difficile la recherche de leurs auteurs. Il permet, à l'inverse, de lever les soupçons pesant sur des personnes suspectées, à tort, d'y être impliquées »*[37]. Il a ensuite constaté qu' *« il résulte de la jurisprudence de la Cour de justice que la directive ne s'oppose pas à une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au*

[35] *Ibid.*, points 37 à 41.
[36] *Ibid.*, points 43 à 46.
[37] *Ibid.*, point 50.

strict nécessaire, mais renouvelable, en vue de lutter contre la criminalité grave ou de prévenir des menaces graves contre la sécurité publique »[38].

Pour ces infractions, le Conseil d'État a toutefois considéré que la solution suggérée par la CJUE d'une conservation ciblée en amont des données *« se heurte à des obstacles techniques qui en compromettent manifestement la mise en œuvre »*[39]. *« En outre*, précise-t-il, *une conservation ciblée, à la supposer techniquement possible, présenterait un intérêt opérationnel particulièrement incertain, dès lors qu'elle ne permettrait pas, y compris en cas de faits particulièrement graves, d'accéder aux données de connexion d'une personne suspectée d'une infraction qui n'aurait pas été préalablement identifiée comme étant susceptible de commettre un tel acte »*[40].

Enfin, il a précisé que, pour garantir le respect des objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs des infractions pénales, la technique de *« conservation rapide »* (*« quick freeze »*), prévue par la convention sur la cybercriminalité signée à Budapest le 23 novembre 2001, permet de protéger la conservation et l'intégrité des données nécessaires à la poursuite de ces finalités pendant une durée de quatre-vingt-dix jours renouvelable, y compris lorsque cette conservation porte sur des données initialement conservées aux fins de sauvegarde de la sécurité nationale. Il en a déduit que *« lorsqu'est en cause une infraction suffisamment grave pour justifier l'ingérence dans la vie privée induite par la conservation des données de connexion, dans le respect du principe de proportionnalité rappelé aux points 38 et 39, l'autorité judiciaire peut, sans méconnaître ni la directive du 12 juillet 2002, ni le RGPD, enjoindre aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs de sites internet de procéder à la conservation rapide des données de trafic et de localisation qu'ils détiennent, soit pour leurs besoins propres, soit au titre d'une obligation de conservation imposée aux fins de sauvegarde de la sécurité nationale »*[41].

Au total, le Conseil d'État a jugé que *« ni l'accès aux données de connexion conservées volontairement par les opérateurs, ni la possibilité de leur imposer une obligation de conservation ciblée, ni le recours à la technique de la conservation rapide ne permettent, par eux-mêmes, de garantir le respect des objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public, notamment celle des atteintes à la sécurité des personnes et des biens, ainsi que de recherche des auteurs d'infractions, notamment pénales »*[42].

---

[38] *Ibid.*, point 52.
[39] *Ibid.*, point 53.
[40] *Ibid.*, point 54.
[41] *Ibid.*, point 55.
[42] *Ibid.*, point 57.

Toutefois, pour aboutir à la conclusion que ces exigences constitutionnelles n'étaient pas pour autant privées de garanties effectives, il a aussitôt relevé que, *« d'une part, à la date de la présente décision, l'état des menaces pesant sur la sécurité nationale rappelées au point 44 justifie légalement que soit imposée aux opérateurs la conservation générale et indifférenciée des données de connexion. D'autre part, la conservation rapide des données susceptibles de contribuer à la recherche, la constatation et la poursuite des infractions pénales, dans le respect du principe de proportionnalité prévu par le code de procédure pénale conformément à ce qui a été rappelé au point 39, est possible dans les conditions prévues par la directive du 12 juillet 2002 et le RGPD, y compris, comme l'a jugé la Cour ainsi qu'il a été rappelé au point 55, lorsque cette conservation rapide porte sur des données initialement conservées aux fins de sauvegarde de la sécurité nationale. L'autorité judiciaire est donc en mesure d'accéder aux données nécessaires à la poursuite et à la recherche des auteurs d'infractions pénales dont la gravité le justifie »*[43].

En conséquence, le Conseil d'État a jugé que *« le Gouvernement ne pouvait pas imposer aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs la conservation généralisée et indifférenciée des données de connexion, autres que les données […] relatives à l'identité civile, aux adresses IP et aux informations relatives aux comptes et aux paiements, aux fins de lutte contre la criminalité et de prévention des menaces à l'ordre public sans méconnaître le droit de l'Union européenne. Il ressort du point précédent qu'à la date de la présente décision, et aussi longtemps que l'existence d'une menace grave sur la sécurité nationale justifie la conservation généralisée et indifférenciée des données de connexion, l'application du droit de l'Union européenne, en conduisant à écarter le droit national, ne prive pas de garanties effectives les objectifs de valeur constitutionnelle invoqués par le Premier ministre en défense. Il y a dès lors lieu d'écarter les articles L. 34-1 du code des postes et des communications électroniques et 6 de la loi du 21 juin 2004 en tant qu'ils poursuivent une finalité autre que celle de la sauvegarde de la sécurité nationale »*[44].

---

[43] *Ibid.* Comme le relevait M. Alexandre Lallet, dans ses conclusions sur cette décision, cette solution constitue une forme de *« "déclassement" du motif de conservation, qui apparaît justifié dès l'instant que la conservation rapide n'est pas elle-même généralisée et indifférenciée, mais porte sur des personnes ou des infractions bien identifiées – c'est la logique du bassin de rétention. Ainsi articulée avec le régime de conservation pour les besoins de la sécurité nationale, la conservation rapide pourra porter non seulement sur les données futures, mais aussi sur les données passées, avec la même profondeur d'un an, et avec le champ d'application large admis par la Cour qui permet de geler les données des suspects, des victimes ou des tiers dès l'instant qu'elles peuvent contribuer à l'élucidation de l'infraction, mais aussi de sanctuariser les données se rapportant à telle ou telle zone géographique – par exemple la liste des numéros de téléphone ayant "borné" dans un secteur ».*

[44] *Ibid.*, point 58.

En définitive, le Conseil d'État a donc jugé que la conservation généralisée et indifférenciée des données de connexion aux fins de lutte contre la criminalité et de prévention des menaces à l'ordre public constituait une garantie des objectifs de prévention des atteintes à l'ordre public. Il n'a accepté de juger cette conservation incompatible avec les exigences européennes qu'aussi longtemps que, dans les faits, ces données continueraient d'être conservées pour la sauvegarde de la sécurité nationale et donc accessibles pour la lutte contre la criminalité et de prévention des menaces à l'ordre public.

* Le Conseil d'État a dès lors enjoint au Premier ministre de procéder à l'abrogation de l'article R. 10-13 du CPCE et du décret du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, en tant que ces dispositions réglementaires :

– d'une part, ne limitent pas les finalités de l'obligation de conservation généralisée et indifférenciée des données de trafic et de localisation autres que les données d'identité civile, les coordonnées de contact et de paiement, les données relatives aux contrats et aux comptes et les adresses IP à la sauvegarde de la sécurité nationale ;

– et, d'autre part, ne prévoient pas un réexamen périodique de l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale.

B. – Origine de la QPC et question posée

Interpellés à la suite de l'exploitation de données de connexion les concernant, MM. Habib A. (QPC n° 2021-976) et Samy B. (QPC n° 2021-977) avaient été mis en examen pour plusieurs infractions de nature criminelle et placés en détention provisoire. Ils avaient tous deux déposé une requête en nullité des actes de procédure ayant permis de requérir, d'obtenir et d'exploiter leurs données de trafic et de localisation.

La chambre de l'instruction de la cour d'appel de Paris avait rejeté leur requête. Ils avaient en conséquence formé un pourvoi en cassation à l'occasion duquel ils avaient chacun soulevé une QPC rédigée en des termes identiques : *« L'article L. 34-1, II et III, du code des postes et des communications électroniques, dans sa version en vigueur du 20 décembre 2013 au 31 juillet 2021, qui autorise pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, la conservation généralisée et indifférenciée pendant un an des données à caractère personnel prévues à l'article R. 10-13 du même code, sans réserver une telle conservation aux infractions les plus graves ni la soumettre à l'autorisation et au contrôle d'une autorité ou juridiction indépendante,*

contrevient-il au droit au respect de la vie privée garanti par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 et à l'article 34 de la Constitution ? ».

Dans ses arrêts du 7 décembre 2021 mentionnés ci-dessus, la Cour de cassation avait considéré que ces questions présentaient un caractère sérieux et les avait renvoyées au Conseil constitutionnel, en relevant que : *« En effet, l'article L. 34-1, III, du code des postes et des télécommunications électroniques, dans sa version en vigueur du 20 décembre 2013 au 31 juillet 2021, permet de différer, pour une durée maximale d'un an, les opérations tendant à l'effacement ou à l'anonymisation de certaines catégories de données de connexion, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, dans le but de permettre la mise à disposition de l'autorité judiciaire. / Or, ces dispositions sont susceptibles de constituer une atteinte excessive aux droits et libertés protégés par l'article 2 de la Déclaration des droits de l'homme et du citoyen, du fait que la conservation des données de connexion et leur accès ne sont pas réservés aux infractions les plus graves et ne sont pas soumises à l'autorisation ou au contrôle d'une juridiction ou d'une autorité administrative indépendante dont les décisions présentent un caractère contraignant »*.

II. – L'examen de la constitutionnalité des dispositions contestées

Le Conseil constitutionnel a décidé de joindre les deux QPC pour y statuer par une seule décision (paragr. 1).

Les requérants, rejoints par les parties intervenantes, reprochaient aux dispositions renvoyées d'imposer aux opérateurs de communications électroniques la conservation générale et indifférenciée des données de connexion, sans la réserver à la recherche des infractions les plus graves ni la subordonner à l'autorisation ou au contrôle d'une juridiction ou d'une autorité indépendante. L'une des parties intervenantes ajoutait qu'une telle conservation n'était pas nécessaire en raison de l'existence d'autres moyens d'investigation. Il en résultait selon eux une atteinte disproportionnée au droit au respect de la vie privée, ainsi qu'une méconnaissance du droit de l'Union européenne.

Au vu de ces griefs, le Conseil constitutionnel a jugé que la QPC portait uniquement sur les mots *« la recherche, de la constatation et de la poursuite des infractions pénales »* et *« de l'autorité judiciaire ou »* figurant à la première phrase du paragraphe III de l'article L. 34-1 du code des postes et des communications électroniques (paragr. 5).

A. – La jurisprudence constitutionnelle relative au droit au respect de la vie privée

1. – Le contrôle des fichiers et traitements de données à caractère personnel

Aux termes de l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 : *« Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression »*. La liberté proclamée par cet article implique le respect de la vie privée[45].

* Depuis sa décision n° 2012-652 DC du 22 mars 2012, le Conseil constitutionnel juge de manière constante, en ce qui concerne la mise en œuvre de traitements de données à caractère personnel, que *« la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif »*[46].

Par cette formule de principe, le Conseil a entendu mettre à la fois l'accent sur la nature des données en cause et sur les différentes opérations caractéristiques des traitements de données personnelles, depuis la constitution et l'enrichissement de telles banques de données – généralement sous la forme de fichiers informatiques – à l'usage qui a vocation à en être effectué par les personnels habilités à les consulter ou à obtenir communication des informations qu'elles contiennent.

Dans sa décision n° 2012-652 DC précitée, le Conseil constitutionnel était saisi des dispositions instituant un fichier, comportant des données biométriques ainsi que l'état civil et le domicile du titulaire, destiné à préserver l'intégrité des données nécessaires à la délivrance des titres d'identité et de voyage, sécuriser la délivrance de ces titres et améliorer l'efficacité de la lutte contre la fraude. Il a jugé que, *« compte tenu de son objet, ce traitement de données à caractère personnel est destiné à recueillir les données relatives à la quasi-totalité de la population de nationalité française ; que les données biométriques enregistrées dans ce fichier, notamment les empreintes digitales, étant par elles-mêmes susceptibles d'être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu, sont particulièrement sensibles ; que les caractéristiques techniques de ce fichier définies par les dispositions contestées permettent son interrogation à d'autres fins que la vérification de l'identité d'une personne ; que les dispositions de la loi déférée autorisent la consultation ou l'interrogation de ce fichier non seulement aux fins de délivrance ou de*

[45] Décision n° 99-416 DC du 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*, cons. 45.
[46] Décision n° 2012-652 DC du 22 mars 2012, *Loi relative à la protection de l'identité*, cons. 8.

renouvellement des titres d'identité et de voyage et de vérification de l'identité du possesseur d'un tel titre, mais également à d'autres fins de police administrative ou judiciaire ; / Considérant qu'il résulte de ce qui précède qu'eu égard à la nature des données enregistrées, à l'ampleur de ce traitement, à ses caractéristiques techniques et aux conditions de sa consultation, les dispositions de l'article 5 portent au droit au respect de la vie privée une atteinte qui ne peut être regardée comme proportionnée au but poursuivi »[47].

* Il ressort de la jurisprudence constitutionnelle que, dans le cadre du contrôle de proportionnalité qu'il exerce sur les traitements de données, le Conseil est attentif aux finalités poursuivies, à la nature des données collectées, à la taille du fichier, à ses caractéristiques techniques, aux modalités de conservation des informations qu'il regroupe ainsi qu'aux conditions de sa consultation.

Sur ce fondement, le Conseil a déclaré contraires à la Constitution :

– les dispositions qui créaient un registre national des crédits aux particuliers, destiné à recenser les crédits à la consommation contractés par les personnes physiques pour leurs besoins non professionnels, les incidents de paiement caractérisés liés aux crédits souscrits par ces personnes ainsi que les informations relatives aux situations de surendettement et aux liquidations judiciaires. Le Conseil constitutionnel a relevé en particulier que ce registre était *« destiné à recueillir et à conserver pendant plusieurs années des données précises et détaillées relatives à un grand nombre de personnes physiques débitrices »*, qu'il pouvait *« être consulté à de très nombreuses reprises et dans des circonstances très diverses »*, que les établissements et organismes financiers étaient autorisés *« à utiliser les informations collectées lors de la consultation du registre dans des systèmes de traitement automatisé de données »* et que le législateur n'avait *« pas limité le nombre de personnes employées par ces établissements et organismes susceptibles d'être autorisées à consulter le registre »*[48] ;

– les dispositions du code général des impôts relatives au registre public des trusts, faute pour le législateur d'avoir précisé la qualité et les motifs justifiant la consultation du registre[49] ;

– certaines dispositions relatives au fichier de traitement d'antécédents judiciaires (TAJ) qui privaient les personnes mises en cause dans une procédure pénale, autres que celles ayant fait l'objet d'une décision d'acquittement, de relaxe, de

[47] *Ibid.*, cons. 10 et 11.
[48] Décision n° 2014-690 DC du 13 mars 2014, *Loi relative à la consommation*, cons. 53 à 57.
[49] Décision n° 2016-591 QPC du 21 octobre 2016, *Mme Helen S. (Registre public des trusts)*.

non-lieu ou de classement sans suite, de toute possibilité d'obtenir l'effacement anticipé de leurs données personnelles[50] ;

– certaines dispositions de l'article 154 de la loi de finances pour 2020 autorisant, à titre expérimental et pour une durée de trois ans, les administrations fiscale et douanière à collecter et à traiter de manière automatisée les données personnelles accessibles publiquement sur les sites internet de certains opérateurs de plateformes, aux fins de recherche de manquements et d'infractions en matière fiscale et douanière[51].

Le Conseil a déclaré conformes à la Constitution, le cas échéant sous certaines réserves :

– les dispositions créant un fichier national des contrats d'assurance-vie[52] ;

– les dispositions créant un répertoire des logements locatifs sociaux et de leurs habitants, pour permettre l'élaboration et la mise en œuvre des politiques publiques de l'habitat[53] ;

– le fichier recensant les personnes qui ont contrevenu ou contreviennent aux dispositions des conditions générales de vente ou du règlement intérieur relatives à la sécurité des manifestations sportives[54] ;

– le régime des traitements de données à caractère personnel relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes, mis en œuvre par des personnes collaborant au service public de la justice[55] ;

– la création d'un fichier des ressortissants étrangers se déclarant mineurs non accompagnés, en relevant notamment *« qu'aucune norme constitutionnelle ne s'oppose par principe à ce qu'un traitement automatisé poursuive plusieurs finalités »*[56] ;

[50] Décision n° 2017-670 QPC du 27 octobre 2017, *M. Mikhail P. (Effacement anticipé des données à caractère personnel inscrites dans un fichier de traitement d'antécédents judiciaires)*.
[51] Décision n° 2019-796 DC du 27 décembre 2019, *Loi de finances pour 2020*, paragr. 75 à 96.
[52] Décision n° 2013-684 DC du 29 décembre 2013, *Loi de finances rectificative pour 2013*, cons. 13.
[53] Décision n° 2016-745 DC du 26 janvier 2017, *Loi relative à l'égalité et la citoyenneté*, paragr. 25 à 29.
[54] Décision n° 2017-637 QPC du 16 juin 2017, *Association nationale des supporters (Refus d'accès à une enceinte sportive et fichier d'exclusion)*.
[55] Décision n° 2018-765 DC du 12 juin 2018, *Loi relative à la protection des données personnelles*, paragr. 47 à 53.
[56] Décision n° 2019-797 QPC du 26 juillet 2019, *Unicef France et autres (Création d'un fichier des ressortissants étrangers se déclarant mineurs non accompagnés)*, paragr. 8.

– les dispositions instituant les systèmes d'information *ad hoc* mis en œuvre pour lutter contre la propagation de l'épidémie de covid-19[57].

* Si, en présence de dispositions instituant de tels traitements de données, le Conseil constitutionnel exerce son contrôle en prenant en considération les différentes opérations entourant leur constitution et l'exploitation des informations qu'ils contiennent, il a également fait application de ce contrôle à des dispositions portant plus spécifiquement sur l'une des opérations de collecte, d'enregistrement, de conservation, de consultation ou encore de communication.

Le Conseil a, en particulier, été amené à se prononcer sur la question particulière de la durée de conservation de données personnelles au sein de fichiers de police et, plus récemment, des systèmes d'information mis en œuvre dans le cadre de la lutte contre l'épidémie de covid-19.

– Dans sa décision n° 2003-467 DC du 13 mars 2003, le Conseil avait été saisi des dispositions organisant les traitements automatisés de données nominatives utilisés par les services de la police nationale et de la gendarmerie nationale dans le cadre de leurs missions[58], auxquelles il était reproché de méconnaître le droit au respect de la vie privée et d'être entachées d'incompétence négative au motif que le législateur avait renvoyé au pouvoir réglementaire le soin de fixer, en particulier, la durée de conservation des données personnelles. Le Conseil a écarté ces griefs après avoir relevé, notamment, que le traitement des informations nominatives était placé sous le contrôle de l'autorité judiciaire, que des dispositions organisaient l'effacement et la rectification des données personnelles, et que le législateur n'avait pas entendu écarter les garanties prévues par la loi « informatique et libertés » du 6 janvier 1978[59]. Le Conseil a par ailleurs considéré *« qu'aucune norme constitutionnelle ne s'oppose par principe à l'utilisation à des fins administratives de données nominatives recueillies dans le cadre d'activités de police judiciaire »*[60]. Il a cependant émis une réserve d'interprétation sur le fondement du principe fondamental reconnu par les lois de la République en matière de justice pénale des mineurs, afin d'imposer au pouvoir réglementaire de *« déterminer une durée de conservation conciliant, d'une part, la nécessité d'identifier les auteurs d'infractions et, d'autre part, celle de rechercher le relèvement éducatif et moral des mineurs délinquants »*[61].

---

[57] Décision n° 2020-800 DC du 11 mai 2020, *Loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions*, paragr. 61 à 78.

[58] Ces dispositions servaient de base légale aux anciens fichiers instituant un *« système de traitement des infractions constatées »* (STIC) pour la police et un *« système judiciaire de documentation et d'exploitation »* (JUDEX) pour la gendarmerie, qui ont été mutualisés depuis dans le fichier de traitements d'antécédents judiciaires (TAJ).

[59] Décision n° 2003-467 DC du 13 mars 2003, *Loi pour la sécurité intérieure*, cons. 22 à 27.

[60] *Ibid.*, cons. 32.

[61] *Ibid.*, cons. 38.

– Dans sa décision n° 2011-625 DC du 10 mars 2011, le Conseil avait été saisi des dispositions intégrant les règles d'institution de ces fichiers de police aux articles 230-6 à 230-11 du code de procédure pénale (servant désormais de base légale au fichier TAJ). Il les a déclarées conformes à la Constitution sous les mêmes réserves que celles énoncées dans la décision précitée. À cette occasion, il a notamment relevé que la différenciation des règles de conservation des données personnelles prévue en cas de classement sans suite, selon qu'un tel classement était motivé par une insuffisance de charges ou tout autre motif, *« est fondée sur l'absence d'intérêt de conserver, dans ce [premier] cas, de telles données dans le fichier »*[62].

En revanche, dans cette même décision, le Conseil constitutionnel a censuré la disposition qui permettait aux enquêteurs par un nouvel acte d'enregistrement de prolonger, au-delà de trois ans, la conservation des données personnelles révélées par l'exploitation des enquêtes et des investigations réalisées au moyen de logiciels de rapprochement judiciaire[63].

– Dans sa décision n° 2017-670 QPC du 27 octobre 2017, le Conseil a de nouveau été amené à se prononcer sur les dispositions organisant la base légale du fichier TAJ, s'agissant plus précisément des conditions dans lesquelles pouvait être demandé l'effacement anticipé des données personnelles figurant dans ce fichier.

Après avoir rappelé que ces dispositions poursuivaient les objectifs de valeur constitutionnelle de recherche des auteurs d'infractions et de prévention des atteintes à l'ordre public, en ce qu'elles visaient à confier aux services compétents un outil d'aide à l'enquête judiciaire et à certaines enquêtes administratives, le Conseil a toutefois relevé, en premier lieu, que *« le législateur a permis que figurent dans ce fichier des données particulièrement sensibles »*[64].

Il a observé, en deuxième lieu, que les fichiers d'antécédents judiciaires étaient *« susceptibles de porter sur un grand nombre de personnes dans la mesure où y figurent des informations concernant toutes les personnes mises en cause pour un crime, un délit et certaines contraventions de la cinquième classe »*[65].

Le Conseil a ajouté, en troisième lieu, que *« le législateur n'a[vait] pas fixé la durée maximum de conservation des informations enregistrées dans un fichier d'antécédents judiciaires. Ainsi, l'article R. 40-27 du code de procédure pénale*

[62] Décision n° 2011-625 DC du 10 mars 2011, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure*, cons. 12.
[63] *Ibid.*, cons. 72.
[64] Décision n° 2017-670 QPC du 27 octobre 2017 précitée, paragr. 10.
[65] *Ibid.*, paragr. 11.

prévoit qu'elles sont conservées pendant une durée comprise entre cinq ans et quarante ans selon l'âge de l'individu et la nature de l'infraction »[66].

En dernier lieu, il a insisté sur le fait que *« ces informations peuvent être consultées non seulement aux fins de constatation des infractions à la loi pénale, de rassemblement des preuves de ces infractions et de recherche de leurs auteurs, mais également à d'autres fins de police administrative »*[67].

Dans ces conditions, le Conseil constitutionnel a jugé qu'en privant les personnes mises en cause dans une procédure pénale, autres que celles ayant fait l'objet d'une décision d'acquittement, de relaxe, de non-lieu ou de classement sans suite, de toute possibilité d'obtenir l'effacement de leurs données personnelles inscrites dans le fichier des antécédents judiciaires, les dispositions contestées portaient une atteinte disproportionnée au droit au respect de la vie privée.

– Dans sa décision n° 2018-765 DC du 12 juin 2018, le Conseil a statué sur les modifications apportées par le législateur à ces mêmes dispositions, à la suite de la censure prononcée dans la décision précitée. Après avoir rappelé que ces dispositions poursuivaient les objectifs de valeur constitutionnelle de recherche des auteurs d'infractions et de prévention des atteintes à l'ordre public, il a de nouveau relevé que *« figurent dans ce fichier des données particulièrement sensibles pouvant être consultées non seulement aux fins de constatation des infractions à la loi pénale, de rassemblement des preuves de ces infractions et de recherche de leurs auteurs, mais également à d'autres fins de police administrative. Par ailleurs, le législateur n'a pas fixé la durée maximum de conservation des informations enregistrées »*[68].

Pour écarter le grief tiré de la méconnaissance du droit au respect de la vie privée, le Conseil a toutefois tenu compte des prérogatives reconnues aux personnes enregistrées dans ce fichier ainsi qu'au juge pénal aux fins d'effacement des données : *« d'une part, les dispositions contestées permettent à toute personne ayant bénéficié d'une décision définitive de relaxe, d'acquittement, de condamnation avec dispense de peine ou de mention au casier judiciaire, de non-lieu ou de classement sans suite, de demander sans délai l'effacement ou la rectification des données la concernant. D'autre part, en l'absence d'une telle décision, la personne peut demander l'effacement ou la rectification des données dès lors qu'il ne figure plus aucune mention de nature pénale dans le bulletin n° 2 de son casier judiciaire. Indépendamment des règles légales de retrait des mentions d'une condamnation au bulletin n° 2, le juge pénal peut exclure expressément une telle mention lorsqu'il prononce cette condamnation ou par*

[66] *Ibid.*, paragr. 12.
[67] *Ibid.*, paragr. 13.
[68] Décision n° 2018-765 DC du 12 juin 2018 précitée, paragr. 81.

jugement rendu postérieurement sur la requête du condamné. Enfin, la mention est supprimée en cas de réhabilitation acquise de plein droit ou de réhabilitation judiciaire »[69].

– Dernièrement, dans sa décision n° 2021-819 DC du 31 mai 2021, le Conseil constitutionnel a examiné les dispositions organisant le transfert, au sein du système national des données de santé (SNDS), des données médicales recueillies à partir des systèmes d'information institués par l'article 11 de la loi n° 2020-546 du 11 mai 2020 au titre de la lutte contre l'épidémie de covid-19[70].

Pour rappel, ces systèmes d'information peuvent comporter des données sur l'identité et l'état de santé des personnes infectées ou présentant un risque d'infection. Le législateur a prévu, par dérogation au principe du secret médical, que ces données puissent être traitées et partagées, le cas échéant, sans le consentement des personnes intéressées. Un grand nombre de professionnels de santé peuvent accéder à ces données, dans la stricte mesure où leur intervention sert ces finalités.

Après avoir réaffirmé la *« particulière vigilance »* qui doit être observée lorsque sont en cause des données de nature médicale, le Conseil a relevé que les données à caractère personnel ainsi collectées ne peuvent, en principe, être conservées à l'issue d'une durée de trois mois[71].

Le Conseil constitutionnel a ensuite observé que le rassemblement de ces données au sein du SNDS et leur soumission aux dispositions du code de la santé publique conduiraient à une augmentation non seulement de la durée de conservation de ces données (*« pour une durée maximale de vingt ans après leur transfert »*), mais aussi du champ des personnes autorisées à y accéder[72].

Reprenant l'articulation classique du raisonnement qu'il avait tenu lors de l'examen de la loi du 11 mai 2020 précitée, le Conseil a alors examiné l'objectif poursuivi par le législateur et analysé l'adéquation et la proportionnalité, au regard de cet objectif, des finalités assignées au traitement, et de l'étendue des données retenues et du champ des personnes ayant accès au traitement.

---

[69] *Ibid.*

[70] Sur le fondement de ces dispositions, le décret n° 2020-551 du 12 mai 2020 a, d'une part, créé un traitement de données à caractère personnel (système d'information national de dépistage, dénommé « SI-DEP »), dont le responsable est le ministre chargé de la santé et, d'autre part, adapté les systèmes d'information de l'assurance maladie, aux fins de mettre en œuvre un traitement de données de suivi des personnes infectées et des cas contacts, dénommé « Contact Covid », dont le responsable est la Caisse nationale d'assurance maladie.

[71] Décision n° 2021-819 DC du 31 mai 2021, *Loi relative à la gestion de la sortie de crise sanitaire*, paragr. 24 et 25.

[72] *Ibid.*, paragr. 27.

Le Conseil a admis, en premier lieu, que le législateur avait poursuivi l'objectif de valeur constitutionnelle de protection de la santé dès lors que les dispositions contestées visaient à améliorer les connaissances sur le virus responsable de l'épidémie de covid-19, en particulier sur ses effets à long terme, et à renforcer les moyens de lutte contre celle-ci[73].

En deuxième lieu, le Conseil a tenu compte d'une caractéristique propre aux données transférées au sein du SNDS, à savoir le fait qu'il s'agit exclusivement de données « pseudonymisées », c'est-à-dire sous une forme ne comportant aucun élément directement identifiant. Le Conseil a relevé, à cet égard, que le code de la santé publique prévoit que ce système ne contient ni les noms et prénoms des personnes dont les données sont recueillies, ni leur numéro d'inscription au répertoire national d'identification des personnes physiques (leur « numéro de sécurité sociale »), ni leur adresse. Toutefois, par une réserve d'interprétation visant à garantir la pseudonymisation des données transférées au sein du SNDS, le Conseil a jugé que, *« S'agissant des données transférées en application des dispositions contestées, sauf à méconnaître le droit au respect de la vie privée, cette exclusion doit également s'étendre aux coordonnées de contact téléphonique ou électronique des intéressés »*[74].

Le Conseil s'est attaché, en troisième lieu, au champ des personnes pouvant accéder aux informations conservées dans le SNDS. Il a relevé que le code de la santé publique prévoit plusieurs garanties procédurales importantes (déclaration ou autorisation préalable auprès de la Commission nationale de l'informatique et des libertés ; soumission au secret professionnel dont la méconnaissance est pénalement sanctionnée ; protocoles devant assurer la confidentialité et l'intégrité des données et la traçabilité des accès). Par ailleurs, en application de l'article L. 1461-2 du même code, dans le cas particulier où des données font l'objet d'une mise à la disposition du public, elles *« sont traitées pour prendre la forme de statistiques agrégées ou de données individuelles constituées de telle sorte que l'identification, directe ou indirecte, des personnes concernées y est impossible »*[75].

Pour finir, le Conseil a souligné que les dispositions déférées prévoient que les personnes dont les données médicales sont rassemblées et mises à disposition par le SNDS doivent être informées des conséquences qui en résultent s'agissant notamment de leur durée de conservation, des personnes qui y ont accès et des finalités en vue desquelles elles peuvent être traitées. Elles sont également

---

[73] *Ibid.*, paragr. 28.
[74] *Ibid.*, paragr. 31. Le Conseil avait formulé une réserve d'interprétation comparable lors de l'examen des dispositions de la loi du 11 mai 2020 pour les données utilisées à des fins de recherche (décision n° 2020-800 DC du 11 mai 2020, précitée, paragr. 67).
[75] *Ibid.*, paragr. 32.

informées du droit d'opposition dont elles disposent en application de l'article 74 de la loi du 6 janvier 1978. Le Conseil a, en particulier, relevé que si le législateur a prévu que cette information intervienne *« sans délai et par tout moyen »*, il a imposé qu'elle soit *« délivrée individuellement aux personnes dont les données sont collectées à compter de l'entrée en vigueur de la loi déférée »*[76].

2. – Le contrôle opéré en matière d'accès aux données de connexion

Le Conseil juge de manière constante qu'il appartient au législateur d'assurer *« la conciliation entre le respect de la vie privée et d'autres exigences constitutionnelles, telles que la recherche des auteurs d'infractions et la prévention d'atteintes à l'ordre public »*[77].

La notion de *« vie privée »* est entendue par le Conseil constitutionnel comme la sphère d'intimité de chacun. Entrent dans cette sphère les données à caractère personnel, au nombre desquelles figurent les données de connexion.

S'agissant de ces dernières, le Conseil constitutionnel a développé une jurisprudence concernant les droits de communication reconnus à certaines administrations ou autorités publiques. Il exerce sur de tels droits un contrôle renforcé depuis qu'il a opéré un revirement de jurisprudence dans sa décision n° 2015-715 du 5 août 2015[78].

* Avant cette date, le Conseil avait jugé conforme à la Constitution le droit de communication des données de connexion reconnu aux agents de l'Autorité des marchés financiers, de la Hadopi, de l'administration des douanes et du fisc.

Dans sa décision n° 2001-457 DC du 27 décembre 2001[79], il s'était notamment appuyé sur l'ancien article L. 32-3-1 du CPCE, devenu l'article L. 34-1, pour admettre le droit d'accès à de telles données par les agents des douanes, de la direction générale des impôts et de la Commission des opérations de bourse : *« le droit d'accès que [la disposition contestée] ouvre à de telles données, dont la divulgation serait de nature à porter atteinte à la vie privée, ne peut s'exercer que* "dans le cadre de l'article L. 32-3-1 du code des postes et télécommunications" *; que cet article énonce avec précision la nature et les conditions de conservation et de communication de ces informations ; qu'il en résulte, notamment, que les données susceptibles d'être conservées et traitées* "portent exclusivement sur l'identification des personnes utilisatrices de services fournis par les opérateurs et

[76] *Ibid.*, paragr. 33.
[77] Voir par exemple les décisions n° 2011-209 QPC du 17 janvier 2012, *M. Jean-Claude G. (Procédure de dessaisissement d'armes)*, cons. 3, et n° 2021-817 DC du 20 mai 2021, *Loi pour une sécurité globale préservant les libertés*, not. paragr. 88, 114, 135 et 148.
[78] Décision n° 2015-715 DC du 5 août 2015, *Loi pour la croissance, l'activité et l'égalité des chances économiques*.
[79] Décision n° 2001-457 DC du 27 décembre 2001, *Loi de finances rectificative pour 2001*, cons. 6 à 9.

sur les caractéristiques techniques des communications assurées par ces derniers" *;* "qu'elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications" *;* "qu'il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques" *»*[80].

De la même manière, le Conseil constitutionnel avait relevé, au sujet de l'accès administratif aux données de connexion par les services de renseignement, dans sa décision n° 2015-478 QPC du 24 juillet 2015 : *« que, selon les dispositions du VI de l'article L. 34-1 du code des postes et des communications électroniques, les données conservées et traitées portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux et ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications ; que selon le paragraphe II de l'article 6 de la loi du 21 juin 2004, les données conservées sont celles de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires ; qu'ainsi, le législateur a suffisamment défini les données de connexion, qui ne peuvent porter sur le contenu de correspondances ou les informations consultées »*[81].

* Depuis ces décisions, le Conseil a toutefois opéré un revirement de jurisprudence, qui rend compte de la sensibilité particulière des données de connexion.

– Dans sa décision n° 2015-715 DC du 5 août 2015 précitée, le Conseil constitutionnel a eu l'occasion de se prononcer sur une procédure de communication des données de connexion conçue en faveur de l'autorité de la concurrence, sur l'exact modèle du dispositif prévu en faveur des agents des douanes et du fisc, ainsi que de l'AMF et la Hadopi.

Le Conseil constitutionnel a jugé *« que la communication des données de connexion est de nature à porter atteinte au droit au respect de la vie privée de la personne intéressée ; que, si le législateur a réservé à des agents habilités et soumis au respect du secret professionnel le pouvoir d'obtenir ces données et ne leur a pas conféré un pouvoir d'exécution forcée, il n'a assorti la procédure prévue par le 2° de l'article 216 d'aucune autre garantie ; qu'en particulier, le*

[80] *Ibid*., cons. 8.
[81] Décision n° 2015-478 QPC du 24 juillet 2015, *Association French Data Network et autres (Accès administratif aux données de connexion),* cons. 12.

fait que les opérateurs et prestataires ne sont pas tenus de communiquer les données de connexion de leurs clients ne saurait constituer une garantie pour ces derniers ; que, dans ces conditions, le législateur n'a pas assorti la procédure prévue par le 2° de l'article 216 de garanties propres à assurer une conciliation équilibrée entre, d'une part, le droit au respect de la vie privée et, d'autre part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions »[82].

– Dans sa décision n° 2017-646/647 QPC du 21 juillet 2017 relative au droit de communication des enquêteurs de l'AMF, le Conseil constitutionnel a confirmé cette évolution dans la conciliation qu'il opère entre le droit au respect de la vie privée et les objectifs de valeur constitutionnelle de sauvegarde de l'ordre public et de recherche des auteurs d'infractions[83].

– Dans sa décision n° 2017-752 DC du 8 septembre 2017, le Conseil a également censuré, pour des motifs analogues, les dispositions de la loi pour la confiance dans la vie politique qui visaient à permettre à la Haute autorité pour la transparence de la vie publique (HATVP) d'exercer directement le droit de communication de certains documents ou renseignement reconnu par l'article L. 96 G du livre des procédures fiscales[84].

– Dans sa décision n° 2018-764 QPC du 15 février 2019, le Conseil a censuré à l'aune de cette même jurisprudence (dans laquelle il puisa un changement des circonstances) les dispositions de l'article 65 du code des douanes qui accordaient un droit de communication aux agents des douanes, compte tenu de l'insuffisance des garanties qu'elles prévoyaient dans leur rédaction résultant de la loi n° 2016-1918 du 29 décembre 2016 de finances rectificative pour 2016[85].

Comme souligné dans le commentaire de ces décisions, ces censures successives s'inscrivaient dans un mouvement jurisprudentiel plus large (observé à l'époque notamment au niveau européen avec l'arrêt *Tele2 Sverige AB* précité rendu par la CJUE le 21 décembre 2016), ayant élevé les exigences en matière de protection

---

[82] Décision n° 2015-715 DC du 5 août 2015 précitée, cons. 137.

[83] Décision n° 2017-646/647 QPC du 21 juillet 2017, *M. Alexis K. et autre (Droit de communication aux enquêteurs de l'AMF des données de connexion)*, paragr. 9 : après avoir rappelé que *« la communication des données de connexion est de nature à porter atteinte au droit au respect de la vie privée de la personne intéressée »*, le Conseil a censuré la seconde phrase du premier alinéa de l'article L. 621-10 du CMF, considérant que *« si le législateur a réservé à des agents habilités et soumis au respect du secret professionnel le pouvoir d'obtenir ces données dans le cadre d'une enquête et ne leur a pas conféré un pouvoir d'exécution forcée, il n'a assorti la procédure prévue par les dispositions en cause d'aucune autre garantie. Dans ces conditions, le législateur n'a pas entouré la procédure prévue par les dispositions contestées de garanties propres à assurer une conciliation équilibrée entre, d'une part, le droit au respect de la vie privée et, d'autre part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions ».*

[84] Décision n° 2017-752 DC du 8 septembre 2017 précitée, paragr. 83.

[85] Décision n° 2018-764 QPC du 15 février 2019, *M. Paulo M. (Droit de communication aux agents des douanes des données de connexion)*, paragr. 8.

de la vie privée et tiré les conséquences des évolutions techniques : même si les données de connexion n'incluent pas le contenu des conversations ou de la correspondance échangées, elles comportent en effet des informations de plus en plus précises, puisqu'elles permettent la localisation en temps réel de l'utilisateur ou du terminal utilisé. En outre, les capacités de traitement des masses de données ainsi générées ont atteint un niveau permettant de disposer d'un grand nombre d'informations sur les personnes concernées.

– La vigilance du Conseil constitutionnel à l'égard des droits de communication portant sur des données de connexion a été de nouveau confirmée dans sa décision n° 2019-789 QPC du 14 juin 2019. À cette occasion, il a considéré que, à la différence des données bancaires, *« compte tenu de leur nature et des traitements dont elles peuvent faire l'objet, les données de connexion fournissent sur les personnes en cause des informations nombreuses et précises, particulièrement attentatoires à leur vie privée »*. Il a également constaté que ces données ne présentaient *« pas de lien direct avec l'évaluation de la situation de l'intéressé au regard du droit à prestation ou de l'obligation de cotisation »*[86]. Comme le relève le commentaire de cette décision, si l'accès à ces données pouvait être utile pour certaines enquêtes relatives à des faits de fraude, il ne l'était pas nécessairement dans l'exercice habituel du contrôle du droit à prestation ou de l'obligation de cotisation, contrairement à l'accès aux données bancaires retraçant les revenus sur lesquels se fondent le calcul de ces derniers. Pour ces raisons, le Conseil a donc considéré que le législateur n'avait pas entouré la procédure prévue par les dispositions contestées de garanties propres à assurer une conciliation équilibrée entre le droit au respect de la vie privée et la lutte contre la fraude en matière de protection sociale.

Si le raisonnement suivi dans cette décision est, sur le fond, similaire à celui qui avait guidé les précédentes décisions rendues à l'égard des données de connexion, il s'en distingue dans sa teneur dans la mesure où le Conseil a explicitement indiqué en quoi l'accès à ces données ne pouvait, compte tenu de leur nature et des traitements dont elles peuvent faire l'objet, être admis selon les mêmes conditions que l'accès aux données bancaires collectées par les agents compétents des organismes de sécurité sociale. La sensibilité plus grande des données de connexion et le lien moins étroit entre ces données et les finalités du droit de communication expliquent que le Conseil ait adopté à leur égard une position différente de celle retenue pour les données bancaires.

– C'est en exposant ce même raisonnement que le Conseil a censuré, dans sa décision n° 2020-841 QPC du 20 mai 2020, les dispositions conférant un droit de communication général à la Hadopi, qui se caractérisait par son champ

[86] Décision n° 2019-789 QPC du 14 juin 2019, *Mme Hanen S. (Droit de communication des organismes de sécurité sociale)*, paragr. 15.

particulièrement large, incluant *« les données de connexion détenues par les opérateurs de communication électronique »*, alors même que ces données ne présentaient pas nécessairement de lien direct avec le manquement à l'obligation énoncée à l'article L. 336-3 du code de la propriété intellectuelle[87].

– Dernièrement, dans sa décision n° 2021-952 QPC du 3 décembre 2021, le Conseil constitutionnel a été saisi des dispositions permettant aux enquêteurs, sur autorisation du procureur de la République, d'accéder aux données de connexion dans le cadre d'une enquête préliminaire.

Dans le prolongement de ses précédentes décisions, le Conseil a relevé que *« les données de connexion comportent notamment les données relatives à l'identification des personnes, à leur localisation et à leurs contacts téléphoniques et numériques ainsi qu'aux services de communication au public en ligne qu'elles consultent »*. Complétant la formule qu'il avait introduite dans sa décision n°2019-789 QPC précitée, il a jugé que *« Compte tenu de leur nature, de leur diversité et des traitements dont elles peuvent faire l'objet, les données de connexion fournissent sur les personnes en cause ainsi que, le cas échéant, sur des tiers, des informations nombreuses et précises, particulièrement attentatoires à leur vie privée »*[88].

Le Conseil a ensuite constaté que *« la réquisition de ces données est autorisée dans le cadre d'une enquête préliminaire qui peut porter sur tout type d'infraction et qui n'est pas justifiée par l'urgence ni limitée dans le temps »*[89].

Il a dès lors considéré que *« Si ces réquisitions sont soumises à l'autorisation du procureur de la République, magistrat de l'ordre judiciaire auquel il revient […] de contrôler la légalité des moyens mis en œuvre par les enquêteurs et la proportionnalité des actes d'investigation au regard de la nature et de la gravité des faits »*, le législateur n'avait assorti le recours à ces réquisitions de données de connexion d'aucune autre garantie[90].

Ainsi, dans son contrôle du droit de communication de données de connexion, le Conseil s'assure désormais tout particulièrement des garanties prévues et du lien que les données communiquées présentent avec la finalité poursuivie.

---

[87] Décision n° 2020-841 QPC du 20 mai 2020, *La Quadrature du Net et autres (Droit de communication à la Hadopi)*, paragr. 17.
[88] Décision n° 2021-952 QPC du 3 décembre 2021, *M. Omar Y. (Réquisition de données informatiques par le procureur de la République dans le cadre d'une enquête préliminaire)*, paragr. 11.
[89] *Ibid.*, paragr. 12.
[90] *Ibid.*, paragr. 13.

B. – L'application à l'espèce

Alors qu'il avait jusqu'à présent été saisi de dispositions relatives aux données de connexion sous l'angle des droits de communication permettant à certaines autorités administratives ou judiciaires d'y accéder, le Conseil constitutionnel s'est prononcé pour la première fois, dans la décision commentée, sur des dispositions imposant et organisant uniquement la conservation de telles données.

* Compte tenu de la nature de ces données, le Conseil a exercé son contrôle sur le fondement du droit au respect de la vie privée protégé par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 (paragr. 6), après avoir repris sa formule de principe qui met en avant la conciliation qu'il appartient au législateur d'établir entre l'exercice de ce droit et les autres finalités poursuivies par ce dernier. En l'occurrence, le Conseil a rappelé qu'*« Il lui incombe d'assurer la conciliation entre, d'une part, les objectifs de valeur constitutionnelle de sauvegarde de l'ordre public et de recherche des auteurs d'infractions et, d'autre part, le droit au respect de la vie privée »* (paragr. 7).

Le Conseil a ensuite resitué l'objet des dispositions contestées au regard du cadre général de l'article L. 34-1 du CPCE relatif au traitement des données à caractère personnel en vue de la fourniture au public de services de communications électroniques.

Après avoir rappelé que le paragraphe II de cet article prévoit l'obligation pour les opérateurs de communications électroniques d'effacer ou de rendre anonymes les données relatives au trafic enregistrées à l'occasion des communications électroniques dont ils assurent la transmission (paragr. 8), le Conseil a relevé que, par dérogation, les dispositions contestées du paragraphe III de ce même article permettent d'obliger ces opérateurs à *« conserver pendant un an certaines catégories de données de connexion, dont les données de trafic, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, en vue de la mise à disposition de telles données à l'autorité judiciaire »* (paragr. 9).

Le Conseil a jugé qu'en adoptant les dispositions contestées, le législateur avait poursuivi les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions (paragr. 10).

Il a alors vérifié si, au regard de ces objectifs, l'atteinte au droit au respect de la vie privée était proportionnée.

Pour cela, et comme il l'avait, par exemple, fait dernièrement dans sa décision n° 2021-952 QPC précitée, le Conseil constitutionnel a tenu compte, en premier lieu, de l'étendue des données personnelles susceptibles d'être conservées en

application des dispositions contestées. Il a relevé à cet égard que les données de connexion *« portent non seulement sur l'identification des utilisateurs des services de communications électroniques, mais aussi sur la localisation de leurs équipements terminaux de communication, les caractéristiques techniques, la date, l'horaire et la durée des communications ainsi que les données d'identification de leurs destinataires »* (paragr. 11).

Par une formule directement inspirée de sa jurisprudence récente, le Conseil en a déduit que, *« Compte tenu de leur nature, de leur diversité et des traitements dont elles peuvent faire l'objet, ces données fournissent sur ces utilisateurs ainsi que, le cas échéant, sur des tiers, des informations nombreuses et précises, particulièrement attentatoires à leur vie privée »* (même paragr.).

En second lieu, le Conseil a souligné l'étendue de l'atteinte résultant du régime de conservation des données de connexion prévu par les dispositions contestées. Il a constaté, d'une part, que cette conservation s'applique *« de façon générale à tous les utilisateurs des services de communications électroniques »* et, d'autre part, que *« l'obligation de conservation porte indifféremment sur toutes les données de connexion relatives à ces personnes, quelle qu'en soit la sensibilité et sans considération de la nature et de la gravité des infractions susceptibles d'être recherchées »* (paragr. 12).

Dès lors, le Conseil constitutionnel a jugé *« qu'en autorisant la conservation générale et indifférenciée des données de connexion, les dispositions contestées portent une atteinte disproportionnée au droit au respect de la vie privée »* (paragr. 13). Il les a donc déclarées contraires à la Constitution (paragr. 14).

* Les dispositions déclarées contraires à la Constitution n'étant plus en vigueur, il n'y avait pas lieu de s'interroger sur leur abrogation. Concernant les effets que les dispositions avaient produits, le Conseil constitutionnel a jugé que la remise en cause des mesures ayant été prises sur le fondement de ces dispositions méconnaîtrait les objectifs de valeur constitutionnelle de sauvegarde de l'ordre public et de recherche des auteurs d'infractions et aurait ainsi des conséquences manifestement excessives. Il a donc exclu que ces mesures puissent être contestées sur le fondement de cette inconstitutionnalité (paragr. 17).